Domain and SSL (Deprecated)

Contact info

Yueteng | yh958@cornell.edu

SSL Certs Expire on: **March 25th 2022**

Root domain

Root domain is:

```
diaper-project.com
```

(Note: Do NOT use this root domain directly. Instead, use the subdomains (for instance, `xyz.diaper-project.com` under the **Domains to use** table below.

Registered as a free domain (renewable every 12 months) at https://domains.google.com/registrar/diaper-project.com/dns?authuser=4&_ga=2.49913062.1133395760.1674578263-1913509637.1674050734

access using the google email diapertestemail@gmail.com

Domains to use

Domains for backend APIs

Please refer to the tables in Deploy Services on AWS (Deprecated)

For API callers (i.e. frontend web/app)

Choose the domain accordingly, prepend it with http or https, and append it with port number and path.

Domains for frontend website (dashboard)

https://dashboard.diaper-project.com

(If you visit via `http://` (without secure) , you'll be automatically redirected to `https://` (with secure))

Note: More details about this, go to the doc "Deploy React on AWS"

SSL Certificate for https (Skip this as long as you know what is SSL and certs)

The free SSL cert from Let's Encrypt is used for this purpose.

Let's Encrypt website (no need to visit for this purpose, though): https://letsencrypt.org/

Where do we need to use SSL certs?

SSL certs are required wherever there is a `https` and domain (Mind the s at the end)

We currently have 5 https domains

- 4 for backend APIs, as in "Domains for backend APIs" above
- 1 for frontend (dashboard), as in "Domains for frontend website (dashboard)" above

Please refer to the two docs about how to deploy them to find details of using SSL certs.

Tutorial Video:

Tutorial video (named "SSL renew Part 1" and "SSL renew Part 2") are uploaded in this box folder. You will need to ask Liz to share with you for access.

https://cornell.box.com/s/qgq5fpwyen6mos9ndj8f64drksgp9qdx

Tutorial for creating SSL cert (Probably you ONLY need to see the "How to renew?" part)

[Tutorial: Configure SSL/TLS on Amazon Linux 2 - Amazon Elastic Compute Cloud]

(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/SSL-on-amazon-linux-2.html#letsencrypt)

On section "**Certificate automation: Let's Encrypt with Certbot on Amazon Linux 2**", Use this to **instal** `certauto`, but **not to create**

Stop after done `sudo yum install -y certbot python2-certbot-apache`

Do the following steps

- **Start at Step 3 (skip Step 1/2). Replace `./certbot-auto` with `sudo certbot` following this link:** [Generate Wildcard SSL certificate using Let's Encrypt/Certbot | by Saurabh Palande | Medium](https://medium.com/@saurabh6790/generate-wildcard-ssl-certificate-using-lets-encrypt-certbot-273e432794d7)
- Use **the command line below** to create. Note: There can be multiple domains in command, e.g. `-d diaper.cf -d *.diaper.cf` (where * is a wildcard)Note: (The order is important)
- First deploy DNS TXT record under the prompted domain (do so at website of freenom.com > Services > My Domains > Manage Domain > Manage Freenom DNS > Add Records)
- Pause here, and use the website below (MxToolbox) to verify it's been activated (mind the value must be correct) then hit continue (otherwise will fail)
- Note: If you include multiple domains, you will be required to enter multiple DNS TXT records
- Link: [DNS Lookup Text Record - MxToolbox](https://mxtoolbox.com/TXTLookup.aspx)

Command line to use

```
sudo certbot certonly --manual --preferred-challenges=dns --email diapertestemail@gmail.com --server
https://acme-v02.api.letsencrypt.org/directory --agree-tos -d diaper.cf -d *.diaper.cf
```

Cert information

Upon success, you'll see some information similar to below

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/diaper.cf/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/diaper.cf/privkey.pem
   Your certificate will expire on 2021-08-09. To obtain a new or
   tweaked version of this certificate in the future, simply run
   certbot again. To non-interactively renew *all* of your
   certificates, run "certbot renew"
```

As shown above, current SSL cert expires on **2021-12-26 (December 26)** (Must renew by the command given "certbot renew" before expiration; Might need to run with "sudo")

Note SSL cert is a separate thing to register besides domain. These two need to be renewed separately.

How to renew?

Note: You only need to renew on the machine with `certbot` installed, and copy the generated certs to other servers. – If you need to instal first, start with "[Tutorial: Configure SSL/TLS on Amazon Linux 2 - Amazon Elastic Compute Cloud]" above.

Redo the steps under "**Do the following steps**" above; And copy the new cert as in "**Copy cert files to somewhere docker can access and give permission**" below

Copy cert files to somewhere docker can access and give permission

Create a `cert` folder under project path, and copy both .pem files into the folder. Then change the permissions by:

```
sudo chown ec2-user:ec2-user ./certs/*
```

This will allow flask and docker to access the cert files.

For dashboard frontend, refer to the doc Deploy React (Deprecated) to know what to do after renewing SSL on dashboard frontend server.

You followed the steps above and have renewed certs on your laptop—now what?

1. SSH into each server
2. Locate the folder that currently holds the certs you want to update and delete its contents
3. Copy the renewed certs from your laptop into the newly emptied folder using SCP